1. Using Nmap's vulners script: like finding Easter eggs, but with cyber threats!

Nmap’s vulners script is a powerful tool for identifying vulnerabilities on a target host. By leveraging a comprehensive database of known vulnerabilities, this script scans specified ports and services, providing detailed information about potential security issues.

Using the `vulners` script as part of regular security assessments can help organizations maintain robust defenses against emerging threats and ensure their systems remain secure.

Write a bash script that accepts a host as an argument `$1`.
Run the `vulners` script on the specified host, targeting ports `80` followed by `443`.

Depending on the scanned network, the output could change.

```
┌──(maroua)-[~/0x07_nmap_post_port_scan_scripting]
└─🏴 sudo ./1-nmap_vulners.sh scanme.nmap.org
[sudo] password for maroua:
marouaa@campusna:~/holbertonschool-
cyber_security/network_security/0x07_nmap_post_port_scan_scripting$ ./1-
nmap_vulners.sh scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-21 15:51 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds
```

The command:

```
nmap -sV --script nmap-vulners/ $1 -p80,443
```

Explanation:

1. **`nmap`**:
   - Initiates the Nmap network scanning tool.

2. **`-sV`**:
   - Enables **service version detection**.
   - Attempts to determine the version of the services running on open ports.
3. **`--script nmap-vulners/`**:
   - Specifies the use of the `nmap-vulners` script.
   - This script checks detected service versions against the **vulnerability database** to identify known CVEs (Common Vulnerabilities and Exposures).
4. **`$1`**:
   - Represents a **Bash positional parameter**, which should be replaced with the target (e.g., IP address, hostname, or network range) when the command is run.
5. **`-p80,443`**:
   - Restricts the scan to ports **80 (HTTP)** and **443 (HTTPS)**.
   - This improves efficiency by targeting specific ports instead of scanning all open ports.

How It Works:

- Nmap performs a scan on the specified target (`$1`) focusing only on ports **80** and **443**.
- The `nmap-vulners` script checks the versions of services detected by `-sV` and matches them to a database of known vulnerabilities.

Installing the `nmap-vulners` Script:

If the `nmap-vulners` script is not already available, you can download it from GitHub:

```bash
git clone https://github.com/vulnersCom/nmap-vulners.git
sudo cp nmap-vulners/vulners.nse /usr/share/nmap/scripts/
sudo nmap --script-updatedb
```

Example Usage:

Assume the target is **192.168.1.1**:

```
./yourscript.sh 192.168.1.1
```

If `yourscript.sh` contains the command, `$1` will be replaced with `192.168.1.1`.

Sample Output:

```
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd 2.4.49
| vulners:
```

```
|   CVE-2021-41773  5.0     https://vulners.com/cve/CVE-2021-41773
|_  CVE-2021-42013  5.0     https://vulners.com/cve/CVE-2021-42013
443/tcp open  ssl/https
| vulners:
|   No vulnerabilities found
|_  See https://vulners.com for more information
```

Benefits:

1. **Vulnerability Detection**:
   - Quickly find vulnerabilities associated with HTTP and HTTPS services.
2. **Focused Scanning**:
   - By targeting ports 80 and 443, it ensures the scan is efficient.
3. **Automation-Friendly**:
   - Perfect for integration into vulnerability management scripts.

Limitations:

1. **False Positives**:
   - Vulnerability detection is based on the version reported, which might not always reflect actual risk.
2. **Limited to Known Vulnerabilities**:
   - Only finds issues that are already in the vulnerability database.

Improvement Suggestions:

To include more detail or additional checks:

- Combine with other vulnerability scripts:

  ```
  nmap -sV --script vuln,vulners $1 -p80,443
  ```

- Output to a file for later analysis:

  ```
  nmap -sV --script nmap-vulners/ $1 -p80,443 -oN vulners_scan.txt
  ```